(1) Yearly notices on support collected, which are itemized by month of collection and provided to families receiving services under the comprehensive Tribal IV–D program as required in § 309.75(c) of this chapter, to all case participants regarding support collections; and

(2) Reports submitted to OCSE for program monitoring and program performance as required in § 309.170 of this chapter;

(g) Provide automated processes to enable OCSE to monitor Tribal IV–D program operations and to assess program performance through the audit of financial and statistical data maintained by the system; and

(h) Provide security to prevent unauthorized access to, or use of, the data in the system as detailed in § 310.15 of this part.

§ 310.15 What are the safeguards and processes that comprehensive Tribal IV–D agencies must have in place to ensure the security and privacy of Computerized Tribal IV–D Systems and Office Automation?

(a) *Information integrity and security.* The comprehensive Tribal IV–D agency must have safeguards on the integrity, accuracy, completeness, access to, and use of data in the Computerized Tribal IV–D System and Office Automation. Computerized Tribal IV–D Systems and Office Automation should be compliant with the Federal Information Security Management Act, and the Privacy Act. The required safeguards must include written policies and procedures concerning the following:

(1) Periodic evaluations of the system for risk of security and privacy breaches;

(2) Procedures to allow Tribal IV–D personnel controlled access and use of IV–D data, including:

(i) Specifying the data which may be used for particular IV–D program purposes, and the personnel permitted access to such data;

(ii) Permitting access to and use of data for the purpose of exchanging information with State and Tribal agencies administering programs under titles IV–A, IV–E and XIX of the Act to the extent necessary to carry out the comprehensive Tribal IV–D agency's responsibilities with respect to such programs;

(3) Maintenance and control of application software program data;

(4) Mechanisms to back-up and otherwise protect hardware, software, documents, and other communications; and,

(5) Mechanisms to report breaches or suspected breaches of personally identifiable information to the Department of Homeland Security, and to respond to those breaches.

(b) *Monitoring of access.* The comprehensive Tribal IV–D agency must monitor routine access to and use of the Computerized Tribal IV–D System and Office Automation through methods such as audit trails and feedback mechanisms to guard against, and promptly identify, unauthorized access or use;

(c) *Training and information.* The comprehensive Tribal IV–D agency must have procedures to ensure that all personnel, including Tribal IV–D staff and contractors, who may have access to or be required to use confidential program data in the Computerized Tribal IV–D System and Office Automation are adequately trained in security procedures.

(d) *Penalties.* The comprehensive Tribal IV–D agency must have administrative penalties, including dismissal from employment, for unauthorized access to, disclosure or use of confidential information.

Subpart C—Funding for Computerized Tribal IV–D Systems and Office Automation

§ 310.20 What are the conditions for funding the installation, operation, maintenance and enhancement of Computerized Tribal IV–D Systems and Office Automation?

(a) *Conditions that must be met for FFP at the applicable matching rate in § 309.130(c) of this chapter for Computerized Tribal IV–D Systems.* The following conditions must be met to obtain 90 percent FFP in the costs of installation of the Model Tribal IV–D System and FFP at the applicable matching rate under § 309.130(c) of this chapter in the costs of operation, maintenance, and enhancement of a Computerized Tribal IV–D System: